[19]中华人民共和国国家知识产权局

Ref2

[51]Int. Cl[7]

H04L 9/14

[12]发明专利申请公开说明书

[21]申请号 00121544.2

[43]公开日 2002年3月6日

[11]公开号 CN 1338841A

[22]申请日 2000.8.11 [21]申请号 00121544.2

[71]申请人 海南格方网络安全有限公司

地址 100088 北京市海淀区马甸桥冠城南园枫叶阁21A

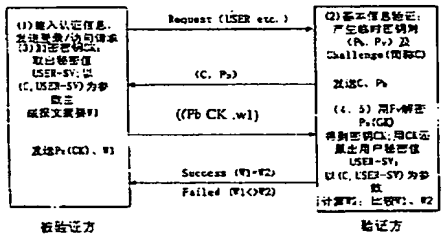
[72]发明人 李志录 何 敏 杨志成

权利要求书1页 说明书4页 附图页数1页

[54]发明名称 计算机安全认证智能密钥

[57]摘要

本发明涉及一种计算机网络身份认证。它主要是对服务器端用户的秘密值采用对称加密算法 进行加密存贮,其加密密钥和原始秘密值保存在该用户的存储介质上;被加密的用户秘密值和加 密密钥分开存贮;又在认证协议验证过程中,引入非对称加密技术,产生临时密钥对,来保证加 密该用户秘密值的密钥传递安全性。从而,实现了安全的身份认证和用户敏感验证信息(秘密信 息)在服务器和客户端的安全存储,防止因超级用户泄漏或复制用户的秘密值的安全隐患。



ISSN1008-4274

知识产权出版社出版

00.08.11

权 利 要 求 书

1、 一种计算机安全认证智能密钥，具有验证方与被验证方共享同样的秘密值和单向加密算法的认证协议，其特征的认证方法：

（1）在注册帐号中，确定好用户名USER，在注册用户中，根据安全认证智能密钥所配的管理工具，在服务器端随机产生一随机的秘密值为USER-SV，利用RC-4算法产生一随机的客户密钥为CK，用CK来加密USER-SV，加密的USER-SV为EN-USER-SV，秘密值USER-SV和客户密钥CK被存放在Skey中，同时设置好Skey保护口令为PIN；而加密的秘密值EN-USER-SV被保存在服务器端；

（2） 客户端本地认证用户对智能密钥Skey持有的合法性的验证，用户把自己注册的Skey插入计算机的USB接口上，启动安全认证智能密钥所带的远程拨号客户端软件，将提示用户输入用户名和PIN值，用户分别输入USER和PIN，Skey将根据用户的输入，在客户端对用户的输入进行检查，只有通过Skey合法性检查以后，才能存取Skey的用户秘密值和用户密钥；

（3） 服务器对用户的认证

① 客户发认证请求和用户名USER给服务器；

② 服务器收到客户的认证请求和用户名USER以后，产生一随机数给客户；同时，产生一对随机的密钥，分别为公钥Pb和私钥Pv，并把公钥Pb送给客户；

③ 客户收到随机数和Pb后，从Skey中读出用户注册的秘密值USER-SV，对客户收到的随机数和USER-SV一起做报文摘要运算，其结果记为W1；同时，客户从Skey中读出客户的密钥CK，利用收到的Pb加密客户密钥CK为Pb-CK；客户把W1和Pb-CK传送给服务器；

④ 服务器收到W1和Pb-CK后，利用服务器随机产生的私钥Pv来解密Pb-CK，其结果为CK；利用CK来解密用户USER的加密的秘密值EN-USER-SV，其结果为USER-SV；利用送给客户的随机数和USER-SV做报文摘要运算，其结果为W2；

⑤ 服务器把收到的W1和产生的W2进行比较，若W1和W2相等，则说明用户合法，否则，用户为非法，若合法，则送成功标志给客户，若非法，则送失败标志给客户；

⑥ 客户收到成功标志，则成功进入系统，否则被拒绝进入系统。

00-00-11

说　明　书

计算机安全认证智能密钥

本发明涉及一种计算机网络身份认证。

众所周知，身份认证在计算机系统和计算机网络中非常重要，目前采用的身份认证方法主要有二种：用户＋口令的方式（如：普通ＰＡＰ认证、人体指纹等生理上的认证方法）、和采用数字证书认证方式。其中第一方式比较适合于不需要经过第三方认证的系统，如：操作系统的用户身份确认、企业内部网络、或借助于互联网络连接的专用网络；而第二种方式则适合于跨部门、跨企业的业务往来，验证的双方是对等的，要相互认证，这种认证需要第三方来确认的双方身份的系统中，如电子商务系统等。

第一种认证方式即为简单的用户名＋口令的方式来认证用户，这种方式存在三大安全隐患：（1）口令易被猜测；（2）口令在网络上传输易被窃获；（3）用户帐号信息被存放在认证方（服务器端），易被超级用户泄密，或被黑客攻击的对象，即使用户帐号信息被加密存放，因加密的密钥和加密的信息被存放在同一台计算机中，总有办法找到加密的密钥来解被加密的信息。

对于用户名＋口令的认证方式一个比较好的改进办法是采用动态密码的认证，其优点是用户每一次的网络登录其密码不一样，杜绝了因在网络上窃听密码而造成系统不安全的可能性。目前，动态密码的认证方式基本上采用安全认证协议，即CHAP(Challenge Handshake Authentication Protocol)。

CHAP是一种通过验证方与被验证方之间的三次信息交互（握手）来验证访问者身份的认证协议。验证方周期性地检验登录和访问请求，一旦检测到，就生成和发送一个随机数Challenge给被验证者。被验证者据此生成一单向加密（One-way encryption）的摘要值作为应答（Response）传给验证方。验证方根据收到的Response来判断用户身份合法性。

CHAP成功认证的前提是验证双方共享同样的秘密值和单向加密算法（One-way Encryption，实际就是HASH算法）。实际验证中，服务器端在发出随机数的同时，会和客户端一道以共享的秘密值和Challenge为因子计算报文摘要，并把二者计算的结果汇总、比较，若相等，则认可该次访问，反之予以拒绝。

CHAP协议能保证用户在验证用户合法性的时候保证每一次登录网上的信息不一样，从而保证用户密码的安全。但其安全性建立在用户/客户机和服务器共享相同的秘密值，为了用户的利益，用户当然会安全地保存自己的秘密值，但服务器秘密值的保存的安全性维系在服务器本身的安全，服务器中秘密值的泄密和破解是本协议的最大安全隐患；另外，CHAP协议本身不能解决用户端口令被猜测的安全隐患。

本发明的目的是提供一种计算机安全认证智能密钥，它虽然要求验证方和被验证方事先共享同一秘密值，但保存的结果却不相同，在提供验证服务的一方是密文，而密钥和明文则交给待验证的用户保管，又为了保证密钥安全传递和用户身份的正确验证，同时使用了非对称和对称加密技术。

本发明的具体构思如下：

1、 利用智能密钥（Skey）和强化的CHAP协议构造安全认证密钥来鉴别用户的身份。

2、 Skey带有独立的处理器，只要插入USB接口，加载不同算法，即可进行各种运算；根据需要，Skey可配置8-64K可擦写存储器（EPROM），足以支持复杂应用的用户信息存储需求；此外，Skey对用户信息采用文件系统管理和双重口令保护，确保信息存取安全可靠。

3、 安全智能认证密钥采用强化的CHAP协议来认证用户，在认证用户过程中，采用CHAP协议来认证用户，但在服务器端用户的秘密值在建立用户帐号是采用随机生成的对称密钥加密存放在服务器端，而密钥被存放在Skey中，由用户自己保存，服务器中不再有用户个人的密钥；而用户自己保存的秘密值无须加密，原始的秘密值被保存在Skey中由用户自己保存；

4、 Skey中用于认证用户身份的秘密值和密钥的提取，必须通过Skey本身的安全认证以后，才能获取。

5、 客户端的密钥传送到服务器，通过服务器端生成的一对随机密钥（公钥和私钥）来保证客户密钥从客户端安全传输到服务器端。首先，服务器把随机的公钥传给客户，客户用这把随机的公钥加密客户密钥，然后，客户把加密的密钥传给服务器，服务器利用随即产生的那对私钥来解密客户密钥。这样，客户密钥被安全地传送到服务器端。

本发明的目的是这样实现的：它具有验证方与被验证方共享同样的秘密值和单向加密算法的认证协议，其特征是：对服务器端用户的秘密值采用对称加密算法进行加密存贮，其加密密钥和原始秘密值保存在该用户的存储介质上；被加密的用户秘密值和加密密钥分开存贮；又在认证协议验证过程中，引入非对称加密技术，产生临时密钥对，来保证加密该用户秘密值的密钥传递安全性。

由于采用上述方案：实现了安全的身份认证和用户敏感验证信息（秘密信息）在服务器和客户端的安全存储，防止因超级用户泄漏或复制用户的秘密值的安全隐患。

下面结合一实施例对本发明作详细的说明。

图1本发明典型实施例框图。

Windows NT远程拨号计算机安全认证智能密钥的使用和认证过程，如图1所示：

（1） NT的用户要到NT系统中注册帐号，在注册帐号中，确定好用户名，如：用户名(USER)，在注册用户中，根据安全认证智能密钥所配的管理工具，在服务器端随机产生一随机的秘密值，记为：USER-SV，利用RC-4算法产生一随机的客户密钥，记为CK，用CK来加密USER-SV，加密的USER-SV，记为EN-USER-SV，秘密值USER-SV和客户密钥CK被存放在Skey中，同时设置好Skey保护口令，记为：PIN，（注：PIN值并不在服务器端保存）；而加密的秘密值EN-USER-SV被保存在服务器端；

（2） 客户端本地认证用户对智能密钥Skey持有的合法性的验证。用户把自己注册的Skey插入计算机的USB接口上，启动安全认证智能密钥所带的远程拨号客户端软件，将提示用户输入用户名和PIN值，用户分别输入USER和PIN，Skey将根据用户的输入，在客户端对用户的输入进行检查，如合法，则进行以下的工作，如不合法，则提示为非法用户，拒绝进入系统。只有通过Skey合法性检查以后，才能存取Skey的用户秘密值和用户密钥。

（3）服务器对用户的认证

① 客户发认证请求和用户名USER给服务器；

② 服务器收到客户的认证请求和用户名USER以后，产生一随机数Challenge给客户；同时，产生一对随机的密钥，分别为公钥和私钥，记为：Pb和Pv，并把公钥Pb送给客户；

③ 客户收到Challenge和Pb后，从Skey中读出用户注册的秘密值USER-SV，对客户收到的Challenge和USER-SV一起做报文摘要运算，其结果记为W1；同时，客户从Skey中读出客户的密钥CK，利用收到的Pb加密客户密钥CK，记为：Pb-CK；客户把W1和Pb-CK传送给服务器；

④ 服务器收到W1和Pb-CK后，利用服务器随机产生的私钥Pv来解密Pb-CK，其结果为CK；利用CK来解密用户USER的加密的秘密值EN-USER-SV，其结果为：USER-SV；利用送给客户的随机数Challenge和USER-SV做报文摘要运算，其结果为W2；

⑤ 服务器把收到的W1和产生的W2进行比较，若W1和W2相等，则说明用户合法，否则，用户为非法。若合法，则送Succed标志给客户，若非法，则送Failed标志给客户；

⑥ 客户收到Succed标志，则成功进入系统，否则被拒绝进入系统。

上述安全智能密钥认证过程可归纳出下列框图：

综上所述本发明的特点如下：

1） 对服务器端用户的秘密值采用对称加密算法进行加密存贮，其加密密钥和原始秘密值保存在该用户的存储介质上（如：Skey、iKey、软盘、智能卡、客户机等）；

2） 被加密的用户秘密值和加密（该秘密值）密钥分开存贮；

3） 在认证协议（CHAP）验证过程中，引入非对称加密技术，产生临时密钥对，来保证加密该用户秘密值的密钥传递的安全性。

综上所述本发明的特点如下：

1） 对服务器端用户的秘密值采用对称加密算法进行加密存贮，其加密密钥和原始秘密值保存在该用户的存储介质上（如：Skey、iKey、软盘、智能卡、客户机等）；

2） 被加密的用户秘密值和加密（该秘密值）密钥分开存贮；

3） 在认证协议（CHAP）验证过程中，引入非对称加密技术，产生临时密钥对，来保证加密该用户秘密值的密钥传递的安全性。

说 明 书 附 图

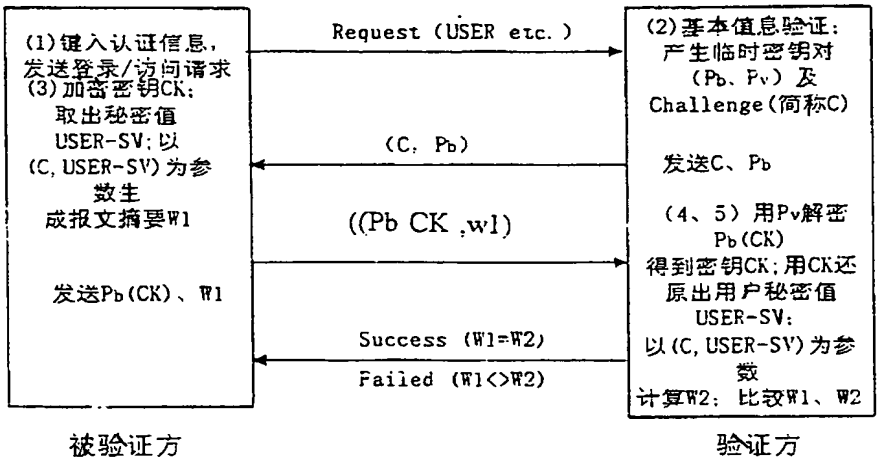

(1)键入认证信息，
发送登录/访问请求
(3)加密密钥CK；
取出秘密值
USER-SV；以
(C, USER-SV)为参
数生
成报文摘要W1
发送Pb(CK)、W1
Request (USER etc.)
(C, Pb)
((Pb CK ,w1)
Success (W1=W2)
Failed (W1<>W2)
(2)基本值息验证：
产生临时密钥对
(Pb、Pv) 及
Challenge(简称C)
发送C、Pb
(4、5) 用Pv解密
Pb(CK)
得到密钥CK；用CK还
原出用户秘密值
USER-SV；
以(C, USER-SV)为参
数
计算W2；比较W1、W2
被验证方
验证方

图 1

CN 1338841A

SMART KEY FOR COMPUTER SECURITY AUTHENTICATION

Abstract

The present invention relates to an identity authentication for computer networks, which applies a symmetric encryption algorithm to secrete values of a server end user so as to be stored in an encrypted form, and stores an encryption key and an original key in a storage medium of the user; separately stores the encrypted user's secret values and the encryption key; and in a course of authenticating with authentication protocols, introduces an asymmetric encryption technique to generate a pair of temporary keys in order to ensure a key transportation security of the user's secrete values. Thus, a secure identity authentication and a secure storage of the user sensitive authentication information (secrete information) in the server and client are achieved, and the possible security problem caused by illegally use of the super-user or the copying of the user's secrete values can be prevented.